NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Visualization and Controls Program Peer Review 2006 Security Metrics for Control Systems

Ron Halbgewachs

Annie McIntyre

Sandia National Laboratories

(505) 284-0968

amcinty@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Work Package Description

- The Security Metrics for Control Systems Work Package was created to address the needs outlined in the Energy Sector Roadmap. Objectives include research on applicability of metrics to control systems, developing a metrics taxonomy, and addressing the use of metrics to benchmark control systems security.
- The overall project goal is to create a taxonomy that an owner/operator can utilize at his or her site to apply cyber security metrics in key operational areas.
- This taxonomy builds on the Automated Systems Reference Model (ASRM) *(Berg, Stamp 2005)* and can clarify difficult aspects of what types of metrics are useful and where they should be applied.

- Budget of $218K

Build a Metrics Taxonomy for Industry with an Operational Focus

Industry Needs

- One of the four fundamental goals delineated within the *Roadmap to Secure Control Systems in the Energy Sector (2005)* is the development of the capability to measure and assess security posture. The document states that reliable and widely-accepted security metrics are needed to enable security posture measurements – need for "Common metrics available for benchmarking security posture".
- Stakeholder's use of actionable metrics is needed to
  - Improve overall security posture
  - Provide situational awareness
  - Assist in procurement decisions
  - Apply resources effectively
  - Define and apply security controls
  - Reduce risk
  - Assist in improving overall operational excellence

Industry Benefits (Impacts)

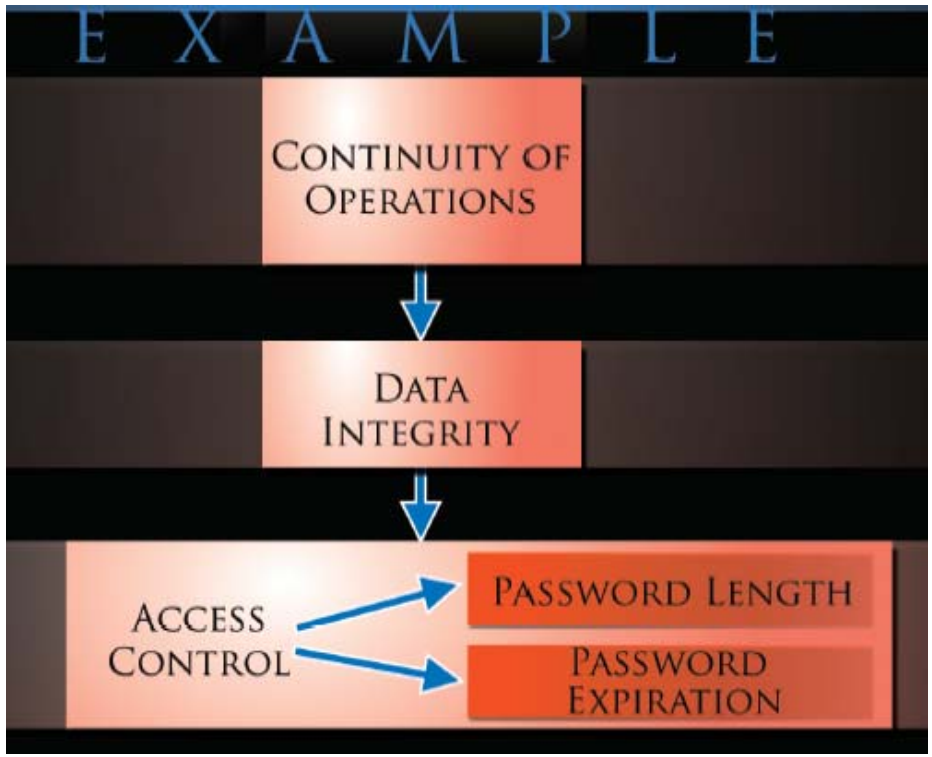
- Metrics assist industry stakeholders in
  - Identifying focus areas within an critical systems architecture
  - Making the business case for procurement and application of resources
  - Employing cyber security controls in appropriate topological areas
- Metrics reduce cyber consequence and risk by providing situational awareness and allow the stakeholder to be proactive rather than reactive, identifying areas subject to risk.
- The Security Metrics for Control Systems Work Package benefits stakeholders by
  - Engaging industry feedback
  - Maintaining an operational focus and holistic approach
  - Taking a flexible approach with a model and taxonomy that can mold to industry needs
  - Creating take-away taxonomy product for industry
  - Building upon multiple standards, and timely due to evolving standards discussions such as API 1164

Technical Approach

- Assess the viability of using security metrics for control systems
  - Determine why metrics are or aren't being employed. What are the barriers?
  - Develop an approach usable for industry, get industry feedback
- Create a metrics taxonomy
  - Create a take-away product for oil, gas, and electric industry.
  - Based a taxonomy upon operational areas and where metrics can be utilized.
  - Utilize and revise the ASRM
  - Define the metrics
- Assess the usage of security metrics for measuring compliance with industry accepted standards and benchmarking security for control systems.
  - Categorize common metrics in existing standards in areas within the model
  - Address where metrics should be applied, cross-referencing those areas with the standards families
  - Address the applicability of using metrics to measure compliance with various standards
- Utilize Information sources:
  - Industry members, Standards bodies, Existing research, Complementary program products, Industry forums
- Coordination/Cross-pollination
  - Monitor activities in the area of metrics, coordinate as applicable. These include academic efforts, industry and government projects and events, and other research and development activities.

Technical Approach

Metrics provide useful data that can be analyzed and utilized in technical, operational, and business decisions across the organization. A metric can be qualitative or quantitative, and is a measurement or reading resulting from an operating state or situation.



Collaborations and Partnerships

- The project has targeted managers in oil, gas, and electric, to increase awareness of metrics and discuss metrics for the business case. Managers and those with the ability to make decisions on the architecture provide information on viability of the approach and taxonomy product. We have asked partners to provide feedback and continue to assist us in refining objectives for maximum utility by industry.

- Tom Frobase – API/Teppco
  - As an executive control systems manager, has provided us with guidance and verified our approach to ensure we create a usable product that includes key pieces. Engaged from the project start. Bridges the gap in understanding API 1164.
- Blake Larsen – Western Refining
  - Provides feedback from an IT perspective as the manager of networks and security. Evaluates methodologies, tool ideas, and approaches for viability and demonstrability.
- NERC Member Body
  - Provides the bulk power perspective and represents an industry that already has the CIP guidelines they are required to follow. Assist us in determining if metrics can help achieve this compliance with standards and/or build inherently more secure systems.
- Discussions on building security and metrics into new programs and addressing incentive opportunities.
  - Alaska Proposed Gas Pipeline Consultant, John Tichotsky
  - DHS Discussion, Perry Pederson
- Other outreach opportunities for feedback
  - SANS, I3P, and PCSF workshops

Technical Progress - Accomplishments

- Solid industry outreach, positive feedback on project
- Created a moldable model that is flexible for industry, rather than a rigid product that may not easily be employed
- Initial research on applicability of metrics for control systems is complete
- Draft metrics taxonomy complete
- Completion of metrics fact sheets and posters
- Completed summary of ongoing metrics efforts
- Coordination of research with I3P Metrics tasks
- Circulated industry questionnaire within API Cybernetics Committee and NERC member body, results are ongoing
- Ongoing interaction/Follow-up visits with industry being scheduled
- On schedule, on budget